известных методов. Предполагается, что дальнейшее развитие данного подхода будет происходить в направлении последовательного адаптивного восстановления характеристик модели среды.

ЛИТЕРАТУРА

1. Park C. B., Miller R. D., Xia J. *Multichannel analysis of surface waves* // Geophysics. – 1999. – V. 64. – P. 800–808.

2. Галимов М. Р., Биряльцев Е. В. *Некоторые технологические аспекты применения высокопроизводительных вычислений на графических процессорах в прикладных программных системах* // Вычисл. мет. и програм. – 2010. – Т. 11. – С. 77–93.

Л. П. Каминский, В. А. Степанов

Сибирский федеральный университет,

kami-lev@yandex.ru, wowchegg@mail.ru

ТРИГОНОМЕТРИЧЕСКАЯ КРИПТОГРАФИЯ

1. Описание работы тригонометрического шифра

Шифр был разработан В.П.Сизовым и успешно представлен на Всероссийскую конференцию “РусКрипто” в 2005 году [1].

Алгоритм шифрования. По координатной оси X расставляются компьютерные символы в любом порядке. Каждому символу соответствует свой порядковый номер от 1 до 256. Всего используется в компьютере 256 символов. По оси Y расставляем те же самые символы в любом (таком же или другом) порядке. Функция, посимвольно переводящая исходный текст

в шифротекст

$$Y = X + 256 \cdot (\cos(Z + N \cdot \Delta x)) \mod 256,$$

где X — порядковый номер того символа который нужно зашифровать; $Z, \Delta x$ – любые числа, являющиеся секретными параметрами нашего ключа. Остальные параметры не являются секретными. $Z, \Delta x \in (-\infty; +\infty)$ N – номер по счету шифруемого символа в исходном тексте; 256 — мощность исходного алфавита. Мощность исходного алфавита может быть любой.

Алгоритм дешифровки. Тригонометрический шифр является примером симметричного алгоритма шифрования, следовательно:

$$X = Y - 256 \cdot (\cos(Z + N \cdot \Delta x)) \mod 256.$$

2. Математические уязвимости и генетический алгоритм

В 2011 году был разработан генетический алгоритм, ставящий под сомнение надежность тригонометрического шифра [2]. В нашем примере мы выбрали косинус, имеющий период 2π. Рассмотрим следующие выражения:

$$\cos((Z + 2\pi) + N \cdot \Delta x) = \cos(Z + N \cdot \Delta x),$$

$$\cos(Z + N \cdot (\Delta x + 2\pi)) = \cos(Z + N \cdot \Delta x).$$

Второе выражение справедливо только для целого N, что выполняется. Таким образом, задача имеет не одно решение, а целое множество, каждое из которых отличается на 2π по любой координате. Это “уязвимое место“ справедливо и для остальных модификаций криптосхемы. Для получения текста, близкого к исходному, в качестве решения можно рассматривать не точку (пару секретных параметров), а некоторую ее

окрестность. Простые практические исследования показали, что в окрестности 10^{-5} в тексте уже легко прослеживается смысл. Этот факт снижает пространство поиска с R^2 до прямоугольника

$$0 < Z < 2\pi, 0 < \Delta x < 2\pi.$$

На нем построим равномерную сетку с шагом $\mathrm{h} = 10^5$. Решениями будут служить точки в узлах сетки. Для их представления потребуется хранить 5 разрядов после запятой по каждой координате. Количество элементов в пространстве решений составит

$$(2\pi \cdot 10^5)^2 \approx 4 \cdot 10^{11}.$$

Однако решить даже такую задачу полным перебором, в отличие от генетического алгоритма, за приемлемое время не представляется возможным.

3. Способы улучшения

На данный момент существует два основных способа улучшения алгоритма тригонометрического шифра:

1) Использование функции с большим периодом, так как период влияет на количество переборов вариантов ключа с нужной точностью. (Период $k\pi$ – количество вариантов ключа пропорционально k^2)

2) Введение третьего параметра ключа. Данное улучшение позволит перейти от плоскости, на осях которой расположены параметры ключа, к объему. Теперь для того, что бы найти тройку параметров с точностью 10^{-5}, потребуется уже не 10^{10}, а 10^{15} переборов.

ЛИТЕРАТУРА

1. Сизов В. П. *Криптографические алгоритмы на основе тригонометрических функций.*

2. Городилов А. Ю., Митраков А. А. *Криптоанализ тригонометрического шифра с помощью генетического алгоритма* // Вест. Пермск. ун-та. – 2011. – № 4(8).

Д. В. Капитанов

Нижегородский государственный университет им. Н. И. Лобачевского,

dis-kdv@mail.ru

ИССЛЕДОВАНИЕ КОЛЕБАНИЙ КОНСОЛЬНО ЗАКРЕПЛЕННОГО СТЕРЖНЯ ПОСЛЕ ПОТЕРИ УСТОЙЧИВОСТИ

Рассматриваются малые низкочастотные плоские изгибные колебания однородного прямого консольно закрепленного стержня с сжимающей продольной нагрузкой на свободном конце. Вывод уравнения и краевых условий осуществляется с использованием принципа Гамильтона-Остроградского [1].

Граница устойчивости определяется при помощи двух различных подходов. Первый подход реализован в виде основанного на методе Бубнова-Галёркина представления проблемы собственных значений с использованием двух первых функций сравнения [2, 3], в результате чего получена система дифференциальных четвёртого порядка уравнений в полных производных. В разработанном алгоритме на каждом шаге малого изменения нагрузки от нуля до некоторого значения система исследуется на устойчивость в соответствии с критерием